Serial Fraud

resistant.ai
Resistant AI Report

The digital transformation has come to fraud

Today's fraudster has ditched confidence and finesse for quantity and persistence. Combining seemingly genuine documents with publicly available editing and automation software, they create floods of documents that overwhelm more than fool their marks. We call the work of these cyber-fraudsters serial fraud. With such a low barrier to entry, business is booming: almost half of companies report being victims of fraud or cybercrime,[1] and successful fraud schemes make off with over $5 trillion worldwide every year from payment providers to online marketplaces and more.[2]

The profits from these attacks are then reinvested into well-organized fraud gangs more like startups than mafias in their structures, technical sophistication, and techniques.[3] Yet traditional anti-fraud solutions don't seem fully aware of this new era of fraud, so most analysts who see serial fraud on the ground aren't equipped to fight the volume and subtlety of documents that characterize it. Resistant AI, however, is specifically built to fight serial fraud. That's why we're pointing out the techniques we see and the unique ways our artificial intelligence stops them.

What we talk about when we talk about serial fraud

You handle document collection and document processors get you the info you need. We sit in between, reducing OCR costs on unreadable or irrelevant documents—and acting as your first line of defense against bad actors.

① Template farms

A Google search can turn up template wizards for nearly any document, from ID cards to PDF bank statements. Upload a photo, provide the desired personal info, and the site spits out an image—even with functioning QR codes or machinereadable zones. Fraudsters can make repeated attempts until a fake slips through or fools human reviewers.

→ The story

A computer whiz wanted to cash in by forging foreign bank statements. Anyone could find their site, pay a few dollars, and specify a name, address, and issuance date. In seconds a legitimate-looking file was ready for download and use across the web, such as inflating "earnings" to secure loans never intended to be repaid. This proved very popular worldwide, with hundreds of examples surfacing.

② Stolen documents

Serial fraudsters can get their hands on legitimate documents and corresponding personally identifiable information through theft, phishing, or buying dark web bundles. Stolen but otherwise genuine documents easily pass through unprepared systems, opening accounts and racking up tabs across the web in the name of real victims.

→ The story

An HR manager decided to take advantage of remote work. Responding to an attractive but fake job offer, applicants sent in their real names, addresses, and other sensitive data. After participating in a recorded Zoom interview, the "new hire" would provide a copy of their ID. With real personal info, a copy of a real ID, and even video material for liveness checks, creating accounts at online shops and services was child's play.

③ Synthetic identities

Synthetic identities fuse the real and the fake. Fraudsters supplement some real documents with some forgeries, or mix and match pieces of information that are individually valid but together don't add up.

→ The story

A homeless shelter's receptionist took advantage of his role and a vulnerable population. Individuals registered at the shelter with an ID card, which the receptionist also used in the first step of the onboarding process of a buy now, pay later (BNPL) service. Once the residents cleaned up, no suspicions were raised during liveness checks. Bank statements forged with the names of the homeless guests completed the BNPL's minimal KYC process. With any number of fake accounts available, this criminal made dozens of expensive fraudulent purchases.

④ Professional forgeries

Far from fabricating "good enough" fakes or scamming at-risk people, professionals know the ins and outs of high-quality fakes and the supporting documentation they need to be accepted without question. With high-quality work and the low risk of operating online, repeated fraud is a no-brainer.

→ The story

A fraud ring contracted a forger to create a fake business from scratch, providing enough resources to enable a thorough job. The result was a series of incorporation documents and invoices that, especially when submitted as photos rather than PDFs, appeared to be proof of a real, long-lived business. Fraudulent seller accounts on dozens of online marketplaces then received thousands from customers for goods and services that never existed

1 "PwC's Global Economic Crime and Fraud Survey 2022" (PricewaterhouseCoopers, 2022)

2 "The Financial Cost of Fraud 2021" (Crowe & University of Portsmouth, 2021)

3 Ben Ellery, "Photoshop fraudsters stand out in £8.5 bn of fake benefit claims" (The Times; 2023)

Serial Fraud

resistant ai
Resistant AI Report

Identify hidden links in high-volume environments

It's not just knowing emerging fraud techniques, it's building tools that catch them. Resistant AI's Document Forensics plugs into your existing document workflow to complement individual document analysis with a simultaneous, real-time look at how one document fits in with every other. Putting documents in context is the core of our unique anti-serial fraud capabilities. Here's how we do it.
Every submitted file is examined by over 500 different indicators, breaking its image characteristics, metadata, and more into points that can be put under a digital microscope.

Many illegitimate documents— around 30% more than by manual review alone—give themselves away here, when letters don't line up, heads don't fit bodies, and so on. But other fakes aren't exposed until these new data points are compared to those from every other submission you've received. Patterns emerge that point to documents being forged in similar ways or to the same document template being reused. Approaching documents as a group with these serial fraud detectors exposes up to 40% more fraud than with individual document analysis alone.

Beyond documents: behaviors

Many companies also gather extra data about who their customers are and how they interact with a service. Including these inputs builds a multi-dimensional picture of who a customer is and how they might be expected to act that is more nuanced than documents alone can provide. Just about anything can act as added submission characteristics: how a user moves through a website, the time they take to complete an onboarding process, what information they submitted as part of a form, the email or phone number they're using, even the type of device being used. These correlations supercharge the already powerful Document Forensics engine—uncovering up to 28% more cases of serial fraud that would have otherwise gone undetected.

Defense in depth and breadth with Resistant AI

By putting more data points under more layers of scrutiny, we evaluate an entire spectrum of the onboarding process at once—not just documents, not just behaviors, but identities. This is how Resistant AI uncovers single entities controlling multiple accounts as well as groups of actors working together.

And this is why a system augmented with our AI can uncover nearly double the number of fraud cases than systems unequipped to counter serial fraud, without adding friction to the customer experience.

+30%
individual documents revealed as fraudulent with Document Forensics over manual review

+40%
fraudulent documents identified by dedicated serial fraud detectors in Document Forensics

+28%
more fraud identified by behavior and submission characteristics

+132%
potential overall uplift in identified fraud with Resistant AI's tools

How we caught them

Now that you know how we combat the latest generation of fraudster, think back to the cases we described above.
How do you think that putting their submissions in context with other documents and with their behaviors gave them away?
Check below to see if you're right.

Template farms

Our template farmer tripped up when his fakes were revealed as inconsistent with the legitimate versions he was trying to replicate.

Stolen documents

Even using genuine info from multiple sources, the "hiring manager" was exposed when shared location and device properties suggested the same person in the same place.

Synthetic identities

The shelter receptionist tipped himself off at numerous points: individual documents were revealed as forgeries and similar photos coming from one location sealed the deal.

Professional forgeries

The professional wasn't good enough. His fakes—despite being many different document types—were taken down because each had been created following the same specific steps.